بسم الله الرحمن الرحيم

**الحمدلله معز الاسلام بنصره ومذل الشرك بقهره ومصرف الامور بأمره ومستدرج الكافرين بمكره، الذي قدر الايام دولا بعدله وجعل العافية للمتقين بفضله والصلاة والسلام علي من أعلي الله منار الاسلام بسيفه وعلي اله وصحبه ومن تبعهم باحسان الي يوم الدين اما بعد..**



## المرحلة الأولي / التصفح الآمن وإخفاء الهوية

الكثير من الأنصار يهملون استخدام شبكة Tor والشبكات الخاصة الإفتراضية اثناء تصفح مواقع التواصل الإجتماعي وذالك من ضمن الاخطاء الفادحة التي يرتكبها الأنصار , فمعظم مواقع شبكة الإنترنت تنتهك خصوصيةالمستخدمين وتحصل علي ملفات تعريف الإرتباط " Cookies " من المتصفح الذي يستخدمونه وملفات تعريف الارتباط هي ملفات نصية صغيرة تستعملها المواقع التي تقوم بزيارتها لحفظ معلومات عنك وتعمل على تخزينها في جهازك وذالك لتعريف هويتك بالنسبة للموقع , إذا كل موقع تتصفحه يخزن ملفات تعريف الارتباط علي جهازك وأيضا يزامن ملفات تعريف الارتباط الاخري مما يكشف هويتك بالنسبة لمواقع التواصل الأخري لذالك ننوه وننصح الأنصار باستخدام جلسات مختلفة لكل موقع و استخدام متصفحات مختلفة وعدم الاعتماد علي متصفح واحد مع تدمير ملفات تعريف الارتباط وسجل التصفح بشكل تلقائي

إن إخفاء الهوية علي شبكة الإنترنت ضرورة حتمية لابد منها لأنصار المجاهدين وذالك لقطع الطريق علي المتربصين بالانصار من تعقبهم وتتبعهم علي شبكة الإنترنت , ومن الادوات التي تعمل علي اخفاء هوية المستخدمين اثناء تصفح شبكة الانترنت متصفح شبكة تور "Tor" حيث يغير عنوان IPالخاص بجهازك والموقع الجغرافي مما يمنحك خصوصية اثناء تصفح شبكة الإنترنت ويمكنك ايضا استخدام الشبكات الخاصة الافتراضية لنفس الغرض ولكن يوجد فرق بين شبكة (Tor) والشبكات الخاصة الافتراضية (VPN)

◂ موقع تويتر يقوم بتسجيل عنوان الIP الخاص بجهازك والموقع الجغرافي في قائمة بياناتك " Your Twitter data " كما موضح في الصورة التالية لذا وجب عليك استخدام متصفح تور "Tor Browser" عند تصفح موقعتويتر فشركة تويتر تسلم بيانات المستخدمين لأجهزة الإستخبارات اذا طلب منها ذالك بشكل قانوني مما يعرض الاخوة الانصار الي الاعتقال في اي وقت - لا قدر الله - بسبب التهاون الأمني علي شبكة الانترنت

Home Notifications Messages Search Twitter

Teston90
@Teston90101

Account
Security and privacy
Password
Cards and shipping
Order history
Mobile
Email notifications
Web notifications
Find friends
Muted accounts
Blocked accounts
Apps
Widgets
Your Twitter data
Accessibility

© 2016 Twitter About Help Terms Privacy Cookies Ads info Brand Blog Status Apps Jobs Advertise Businesses Media Developers

A snapshot of your account information.

Account history

Account creation — Jul 25, 2016 at 8:14 AM (located in Italy)

Username — @Teston90101 Edit

Email — (pending confirmation)

Phone — Add a phone

Login history

If you see any suspicious activity from an app, go to the Apps tab to revoke its access. In some cases the IP location may differ from your physical location. Learn more

| APP | DATE & TIME |
| --- | --- |
| Twitter.com | Jul 25, 2016 8:14 AM |

Other data

Contacts — Manage the contacts imported from your address book.

Twitter Archive — Download your entire Tweet history.

Connected apps — Review the apps that you have given access to your Twitter account

## المرحلة الثانية/حماية حساب تويتر من الإختراق

### أولا : التحقق بخطوتين

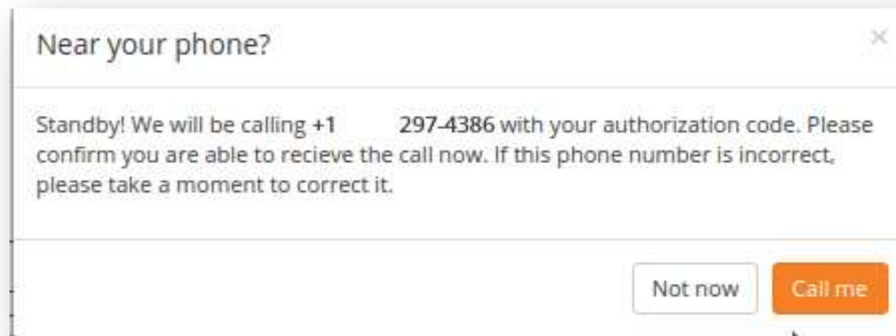
**تفعيل خاصية التحقق بخطوتين في موقع تويتر يضيف طبقة من الحماية الي حسابك حيث يمنع الهكرز من الوصول الي حسابك حتي وإن حصلوا علي كلمة المرور مما يجعل عملية إختراق الانصار أصعب ولكن لتفعيل خاصية التحقق بخطوتين او " توثيق الدخول " يجب عليك اضافة رقم وهمي إلي حساب تويتر لتستقبل اكواد تسجيل الدخول عليه**

شرح إضافة رقم وهمي إلي حسابات تويتر

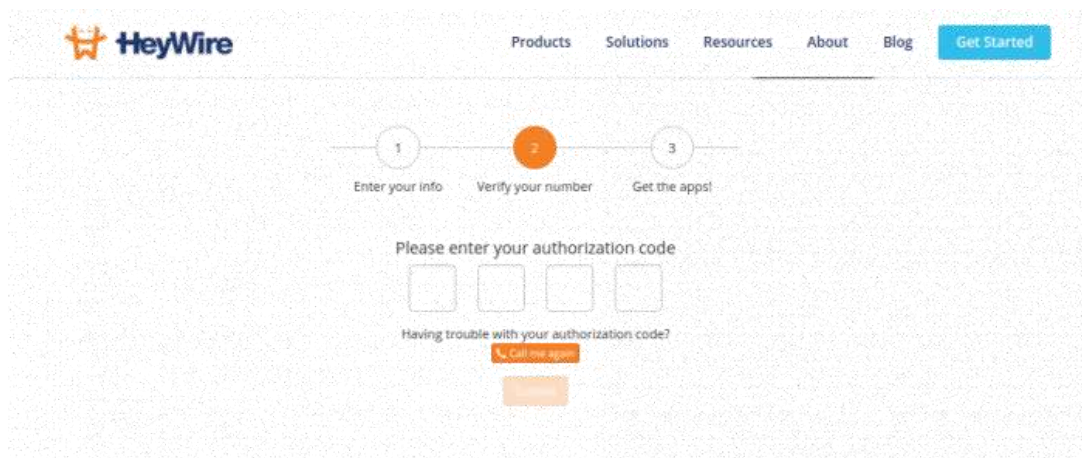
- **حمل تطبيق Talkatone وسجل فيه لتحصل علي رقم أمريكي**
- **سجل بموقع Heywire لتقوم بتفعيل خدمة VOIP برقم Talkatone كما موضح في الصورة التالية**

HeyWire
Products Solutions Resources About Blog Get Started
1 Enter your info
2 Verify your number
3 Get the apps!
Please enter your information
الإسم الأول
الإسم الثاني
البريد الإلكتروني
رقم الهاتف
كلمة المرور
تأكيد كلمة المرور
I'm not a robot
By checking this box, I agree to HeyWire's Terms & Conditions

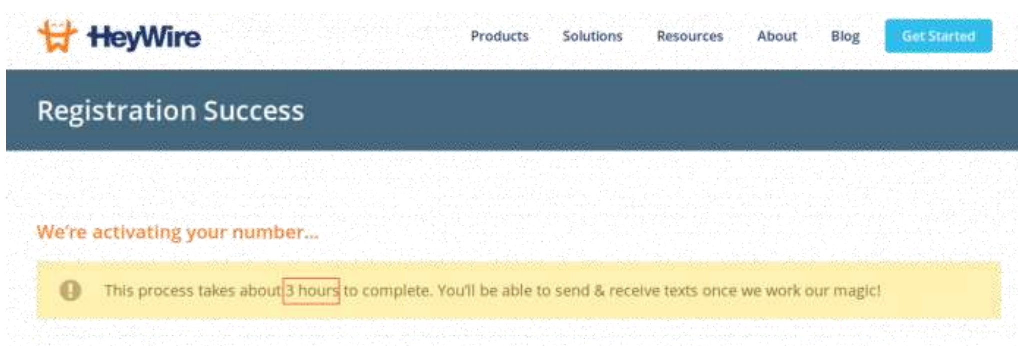
- **أدخل البيانات الموضحة في الصورة التالية**




- إضغط علي Call me لتستقبل مكالمة بها كود التفعيل علي رقم Talkatone




- ادخل الكود ثم اضغط Submit




- بعد 3 ساعات سيتم تفعيل رقم Talkatone علي تطبيق Heywire

- قم بتحميل تطبيق Heywire علي جهازك ثم ادخل الرقم الأمريكي وكلمة المرور وسيبدأ العد التنازلي لبدء استقبال الرسائل والمكالمات الصوتية

## {تفعيل توثيق الدخول}

- إضغط علي صورة الحساب واختر "Settings " من القائمة المنسدلة ثم اضغط Mobile ثم اضف رقم الهاتف الوهمي الذي حصلت عليه من تطبيق Talkatoneكما في الخطوات السابقة

- سيصلك كود التحقق علي تطبيقHeywire بجهازك



- توجه الي اعدادت حساب تويتر واضغط علي Security and Privacy ثم قم بتفعيل خيار " Verify login requests " او توثيق الدخول




- اضغط علي Start وانتظر حتي يرسل تويتر كود توثيق الحساب علي تطبيق Heywire ومن ثم يكون انتهي تفعيل خاصية التحقق بخطوتين في تويتر بنجاح و يكون حسابك محمي من الاختراق بالطرق الشائعة باذن الله

ثانيا : إعدادات الأمان العامة

- تحقق من ضبط إعدادت الحساب كما في الصورة التالية

Home Notifications Messages

Search Twitter

**Teston90**

- Account
- **Security and privacy**
- Password
- Cards and shipping
- Order history
- Mobile
- Email notifications
- Web notifications
- Find friends
- Muted accounts
- Blocked accounts
- Apps
- Widgets
- Your Twitter data
- Accessibility

## Security and privacy

Change your security and privacy settings.

### Security

**Login verification**

☑ Verify login requests

Get Backup Code

Save this backup code to ensure that you can still log in if you ever lose access to your device.

Generate app password

Generate a temporary password to log in to devices and apps that require Twitter credentials.

**Password reset**

☑ Require personal information to reset my password

When you check this box, you will be required to verify additional information before you can request a password reset with just your @username. If you have a phone number on your account, you will be asked to verify that phone number before you can request a password reset with just your email address.

**Log in with code**

○ Allow my account to log in with either a password or login code

You are not eligible for this option because you have enabled login verification. Learn more

◉ Always require a password to log in to my account

You will be asked for your password every time you log in. This means you will not be able to log in by simply receiving a login code (via SMS or email). Learn more

### Privacy

**Photo tagging**

○ Allow anyone to tag me in photos

○ Only allow people I follow to tag me in photos

◉ Do not allow anyone to tag me in photos

**Tweet privacy**

☐ Protect my Tweets

If selected, only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. Learn more

**Tweet location**

☐ Add a location to my Tweets

When you tweet with a location, Twitter stores that location. You can switch location on/off before each Tweet. Learn more

Delete location information

This will delete location labels you have added to your Tweets. This may take up to 30 minutes.

**Discoverability**

☐ Let others find me by my email address

☐ Let others find me by my phone number

**Address book**

Manage your contacts

**Promoted content**

☐ Tailor ads based on information shared by ad partners.

This lets Twitter display ads about things you've already shown interest in. Learn more about how this works and your additional privacy controls.

**Twitter for teams**

○ Allow anyone to add me to their team

○ Only allow people I follow to add me to their team

◉ Do not allow anyone to add me to their team

**Direct Messages**

☐ Receive Direct Messages from anyone

Save changes

## ثالثا : أمان كلمات المرور

1

PASSWORD

# أمان كلمات المرور

تعتبر كلمات المرور خط الدفاع الأول ضد المخترقين فهي الطريقة الرئيسية للحاسوب او الجوال ليثق في مستخدم معين . حيث نستخدم كلمات المرور دائما في حماية انظمة التشغيل والبريد الإلكتروني والبطاقات البنكية وتشفير الملفات وغيرها من البيانات الحساسة . جزء كبير من الحماية يعتمد علي انشاء كلمة مرور قوية وحمايتها .

### إختيار كلمات مرور آمنة :

عند الاعتماد علي كلمة مرور فيجب ان تكون معقدة بالقدر الكافي حتي لا يسهل تخمينها من خلال معرفة بياناتك الشخصية او من خلال هجمات القوة العمياء brute-force .

### كلمات المرور الغير آمنة تحتوي علي هذه البيانات :

- بيانات شخصية مثل تاريخ الميلاد ، المكان ، الاسماء .
- ارقام الهواتف و كلمات شائعة ومشهورة مثل Password .
- عبارات قصيرة اقل من 8 عناصر او كلمات قاموسية .

### تعتمد قوة كلمة المرور علي عنصرين :

العنصر الاول : التعقيد والعشوائية حيث تتكون كلمة المرور الآمنة من مجموعة من العناصر المعقدة كالحروف الصغيرة والكبيرة والارقام والرموز مثل " |aRzAc7<?ZIhF<X'GPW" .

العنصر الثاني : الطول حيث يجب ان يكون طول كلمات المرور من 8 الي 20 عنصر عشوائي .

الوعي الامني

Horizons

2

# أمان كلمات المرور

## عند تعيين كلمة مرور عليك اتباع الشروط التالية:

- اختر كلمة مرور مكونة من 16 عنصر او اكثر .
- استخدم ارقام ورموز مثل $%^&#() ضمن كلمة المرور .
- استخدم الأحرف الصغيرة مثل a b c d و الاحرف الكبيرة مثل A B C D .
- تجنب استخدام العبارات الشهيرة او المستخدمة بكثرة .
- تجنب استخدام معلومات شخصية كالاسم او رقم الهاتف .

## نصائح هامة:

- من الأخطاء الشائعة بين الأنصار استخدام كلمة مرور واحدة لجميع الحسابات والبيانات الحساسة فإن استطاع المهاجم الحصول علي كلمة مرور واحدة يمكنه الوصول لجميع بياناتك الحساسة , لذا عليك بتعيين كلمة مرور مختلفة لكل خدمة علي تستخدمها .
- استخدم برمجيات حرة لتخزين كلمات المرور المعقدة مثل برمجية KeePassX فهي تعتبر خزانة لكلمات المرور وهي برمجية مفتوحة المصدر ومجانية , ان استخدام أدوات لإدارة كلمات المرور يساعدك في اختيار كلمات مرور قوية يصعب علي المهاجم تخمينها حيث تساعد ادوات ادارة كلمات المرور في انشاء كلمات مرور عشوائية غير قابلة للتخمين بدون نمط او هيكل ما .
- استبدل كلمة المرور بأخري جديدة بشكل دوري , وتحقق من عدم وجود برمجيات Keylogger تسجل كل ماتكتبه علي لوحة المفاتيح وذالك من خلال تثبيت برمجية KeyScrambler أو Zemana Anti-logger .
- تحقق من تفعيل خاصية التحقق بخطوتين Two Factor Authentication لمنع المهاجم من الولوج الي حساباتك في حال حصل علي كلمة المرور .
- لا تشارك كلمة المرور مع اي شخص ولا تحتفظ بكلمة المرور داخل ملف علي حاسوبك او جوالك فهذا يعرض سرية كلمات المرور الي الخطر في حال اختراق جهازك .



## المرحلة الثالثة/ تعليمات هامة

- إحذر من الضغط علي روابط مشبوهة من أشخاص مجهولين وافحص الروابط دائما بموقعVirustotal.com قبل الضغط عليها

- تحقق من ان الموقع الذي تتصفحه يستخدم بروتوكول HTTPS حيث يبدأ عنوان موقع الرسمي بهذا البروتوكول

- إحذر من استخدام تطبيق تويتر الرسمي علي نظام iOSو أندرويد - إلا بشروط وضحناها هنا واستخدم متصفح Onion browser او Orfox

- إحرص علي استخدام متصفح تور الرسمي علي انظمة ويندوز وماك ولينكسويونكس وتجنب المتصفحات الشائعة

- تجنب إرسال اي بيانات حساسة او شخصية علي موقع تويتر واستخدم تويتر في نشر الاصدارات وتبصير العوام بحقيقة الصراع فقط

- إحذر من استخدام البريد الإلكتروني المؤقت واستخدم خدمات البريد الإلكتروني المشفرة مثل Protonmail.com

و Tutanota.com و Ghostmail.com

- إحرص دائما علي إستخدام خدمات الشبكات الخاصة الإفتراضية " VPN " اثناء تصفح موقعتويتر ومواقع شبكة الانترنت الأخري

- إحرص علي تثبيت برمجية Keyscrambler و-Zemana Anti logger لتشفير البيانات الحساسة التي تكتبها بلوحة المفاتيح

واخر دعوانا ان الحمدلله رب العالمين

وصلى الله على سيدنا محمد وعلى اله وصحبه وسلم

## للدعم الفني تواصل معنا على

 | **SR444TAW**  | **Tech_Support**


آفاق
Horizons
مؤسسة آفاق الإلكترونية
درع المجاهدين الإلكتروني